5/24/10 (16)

Christine Joyce

From: Merrily Evdokimoff
Sent: Friday, May 14, 2010 12:29 PM
To: Christine Joyce
Subject: Identity Theft Policy for Nursing

Christine,

I am sending an electronic copy of this in case you want to send it out that way. I will bring down 3 copies that need to be signed by clerk after approval and then I need one set for my policy manual. Steve L. mentioned it might go on consent with an introduction as most departments will be having this--we are just the first-lucky us!
Merrily

ACTON PUBLIC HEALTH NURSING SERVICE

SUBJECT: Identity Theft Policy

CHAPTER: LEADERSHIP

A. PURPOSES: The purposes of this Policy are:

1. To help protect employees, patients, customers, contractors and the Town of Acton from damages related to the loss or misuse of personal data.
2. To identify, detect and respond to Red Flags indicating possible Identity Theft related to services offered by the Acton Public Health Nursing Service (the "Nursing Service").
3. To ensure the Nursing Service's compliance with the HIPAA Breach Notification Rule.
4. To ensure that this Policy is updated periodically.

B. DEFINITIONS: For the purposes of this Policy, the following definitions apply:

1. "Breach" means an impermissible use or disclosure under the HIPAA Privacy Rule that compromises the security or privacy of protected health information, posing a risk of financial, reputational, or other harm to the affected individual. A breach does NOT include:
   a. Unintentional access to information by an employee;
   b. Inadvertent disclosure of protected information by the Nursing Service to another party authorized to access it; or
   c. Disclosure of information where the person to whom the disclosure was made would not be able to retain the information.
2. "Business Associate" means an outside business or organization that provides services by agreement or contract to the Nursing Service, including but not limited to billing, accounting, or transportation services.
3. "Identity Theft" means fraud committed or attempted using the identifying information of another person.
4. "Identifying Information" means any name or number that may be used, alone or in conjunction with any other information, to identify a specific person.
5. "Patient" means all customers or consumers of services provided by the Nursing Service.
6. "Protected Health Information" means personally identifiable health information.
7. "Red Flag" means a pattern, practice or specific activity that indicates possible existence of Identity Theft.

C. POLICY:

1. It is the Policy of the Nursing Service to comply with all federal and state laws and reporting requirements regarding Identity Theft.

2. This Policy is designed to protect against and detect the misuse of the following personal data of employees or patients of the Nursing Service (whether in printed or electronic form):
   a. Social Security Number;
   b. Tax, Business or Employer ID Number;
   c. License number;
   d. Credit card information;
   e. Payroll information;
   f. Financial account information;
   g. Protected Health Information (as defined in HIPAA), such as personally identifiable health information contained in medical records or charts;
   h. Date of birth; and
   i. Patient or file number or ID.

3. The Administrator of the Acton Public Health Nursing Service (the "Administrator") or her designee is assigned the responsibility of Compliance Officer, implementing and maintaining this Policy. The Compliance Officer will also receive and process any complaints or concerns from patients regarding personal information. The current Compliance Officer is:

   Name: Merrily Evdokimoff, RN, PhD(c)
   Title: Administrator
   Phone: 978-264-9653
   Email: mevdokimoff@acton-ma.gov
   Address: Town Hall, 472 Main Street, Acton, MA 01720

4. Pursuant to the existing HIPPA Security Rule, appropriate physical, administrative and technical safeguards will be in place to reasonably safeguard protected health information and sensitive information related to patient identity from any intentional or unintentional use or disclosure.

5. All Nursing Service staff were trained to detect and respond to identity theft threats as of January 1, 2010. Thereafter, Nursing Service employees will be trained annually in the implementation of this Policy, and this Policy will be included in the orientation of newly hired employees.

6. The Policy is approved by the Acton Board of Health and Board of Selectmen at inception and will be reviewed annually by the Administrator. Revisions will be recommended to the Board of Health and the Board of Selectmen

annually for approval. Updates to this Policy will then be distributed to employees and Business Associates of the Nursing Service.

7. It is the Nursing Service's Policy that all Business Associates will be contractually bound (a) to comply with FTC Red Flags Rule, any applicable state law concerning data security and this Policy, and (b) to have policies in place to detect, prevent and mitigate the risk of Identity Theft. The Compliance Officer will confirm the existence of these policies with each contact person at each Business Associate.

8. The Compliance Officer will work with the Town's Director of Information Technology to ensure that all electronically stored Protected Health Information is password protected. The Compliance Officer will also ensure that all Protected Health Information sent electronically or stored on portable devices is encrypted.

D. PROCEDURE:

1. Identification of Red Flags:

A. In the course of caring for patients, staff may encounter inconsistent or suspicious documents, information or activities that may signal Identity Theft.

B. The Nursing Service has identified the following Red Flags that may occur in the course of providing services:

1. Alerts, notifications or warnings are received from a consumer or credit reporting agency, including an unusual increase in use.
2. A complaint or question is made by a patient based on the patient's receipt of:
    i. A bill for another individual;
    ii. A bill for a product or service that the patient denies receiving;
    iii. A bill from a health care provider that the patient never patronized;
    iv. An explanation of insurance benefits (EOB) for health care services never received; or
    v. Records indicating medical treatment inconsistent with current findings for example allergies are inconsistent.
3. Records show medical treatment that is inconsistent with a physical examination or a medical history as reported by the patient or healthcare provider.
4. An insurance report indicates that insurance benefits have been depleted or the lifetime cap has been reached.
5. A patient who claims to be a victim of Identity Fraud disputes a bill.

6. A patient is unable to produce an insurance card (in conjunction with other Red Flags).
7. A notice or inquiry is received from an insurance fraud investigator for a private health insurer or a law enforcement agency, including a Medicare or Medicaid fraud agency.
8. Mail sent to the identified patient is repeatedly returned as undeliverable.
9. Inconsistent information is noted on identifying documents presented by the patient including, but not limited to:
    i. Documents appear to have been altered or forged;
    ii. Addresses do not match;
    iii. Social Security numbers have not been issued or are listed on the Social Security Administration's Death Master File;
    iv. Addresses given are typically associated with fraudulent activities such as mail drops or prison addresses;
    v. Out of area phone numbers are provided where there is no accompanying information to explain use of such number; or
    vi. Incomplete personal information is provided on applications.

2. **Detection of Red Flags**

A. Any request for services made directly by a family member of a patient or potential patient must be confirmed in writing by an ordering physician.

B. Upon first undertaking care from the Nursing Service, two forms of patient ID are required to be shown to the attending clinician: one picture ID and one health insurance card. If patient is unable to produce one of these forms of ID, confirmation of identity by another agency employee or verification from Town of Acton Town Clerk's office of residence may suffice.

C. In reviewing ID presented, the attending clinician will look for the Red Flags identified above.

D. An alternative procedure for confirming identity will be determined by the attending clinician and the Compliance Officer, should they be unable to utilize above methods.

E. If the patient has received Nursing Service care previously and is known to employees, this step may be waived.

F. If patient has not completed registration form within past six months, review form with the patient to make sure it is up to date.

G. All Nursing Service employees will review all identifying information upon receipt from each patient to ensure that there are no inconsistencies.

H. All Nursing Service employees are required to report any suspicion of fraud or abuse to the Compliance Officer.

3. **Response to Red Flags**

A. Employees are required to immediately report all Red Flags to the Compliance Officer, along with all related documentation and complete an Unusual Occurrence Report, a sample of which is attached to this Policy as Exhibit A.

B. All breaches of security, such as loss of laptop containing patient information must be reported to Compliance Officer immediately.

C. If the Nursing Service employee detects any discrepancies or is unable to complete identification procedure, the employee is instructed not to raise alarm, but to record any documentation available, complete admission to the extent possible and leave the residence. The employee is not to confront anyone in their home regarding the concerns.

D. Upon receipt of the documentation and an Unusual Occurrence Report, the Compliance Officer will review all materials and authenticate the documentation (to the extent possible) to determine whether fraudulent activity or other potential Breach has occurred.

E. If fraudulent activity or other potential Breach is detected, the Compliance Officer will take the following steps:

   i. Determine if a Breach has occurred (as defined in Section B.1 above).
      a. For guidance on whether a breach has occurred, refer to the Breach Assessment Tool, attached as Exhibit B to this Policy.
   ii. If there is a Breach,
      a. Cancel all pending transactions.
      b. Check the affected patient charts to make sure no fraudulent information was added to charts that may compromise patient health and safety.
         1. Maintain the separate chart with false or fraudulent information. This may be necessary for cross-reference to affected patient's chart and may aid in further investigation of the Breach.
      c. Initiate the applicable notification requirements described below. [Note: The notification requirements are only triggered in the event of a Breach involving *unsecured* (meaning non-encrypted) personal information as listed in Section C.2 above.]

4. **Notification Requirements in Case of a Breach:**

A. In case of a Breach, the Compliance Officer will notify the Town Manager (Steven Ledoux, 978-264-9612) and Town Counsel (Stephen Anderson, 617-621-6510), explain relevant facts and identify steps already taken in relation to Breach.

B. Notify Acton Police Department:

i. In case of a Breach, the Compliance Officer will call Chief of Police at (978) 264-9638 as soon as possible. The conversation with the Police Chief should cover the following:

a. Documents required by Police to investigate the suspicious activity. (Note: Do not provide confidential health information. Do provide information necessary to further investigation.)

b. Whether notification of affected patients should be delayed due to the Police investigation. If Police recommend delay, that request should be in writing and provide a rationale for delay.

C. Notify the Affected Patient

i. The Compliance Officer will provide written notification to the affected patient within 60 days by first class mail, *unless instructed otherwise by federal, state or local police or law enforcement officials*. Notice of any such instructions should be provided by the Nursing Service to Town Counsel.

ii. If the patient has asked for notification by email, provide notification by email. Nursing Service must retain a copy of all written notifications made under this rule for at least seven years.

iii. If the patient is deceased, the Compliance Officer will notify next of kin, if known.

iv. If the Nursing Service does not have contact information for 10 or more patients affected by any Breach, the Compliance Officer will post a notice of the Breach on the Nursing Service website or follow media notification procedures described below.

v. A sample notification letter is attached to this Policy as Exhibit C. The Compliance Officer should modify this letter as needed on a case by case basis. In any event, any notification should include:

a. A brief description of the Breach including the date of the Breach and the date of discovery (if it is known).

b. A description of the types of data or information involved:

1. Include details about the categories of information that have been accessed or acquired (Social Security number, financial data, etc.).

2. Do not include technical details as to how data was obtained as this may further compromise security.

c. A description of the possible level of threat to the affected patient.

d. Steps the patient can take to protect him or herself. Instructions for obtaining a credit report freeze and to obtain credit reports (as shown in the attached sample letter) and a copy of *Medical Identity Theft Response Checklist for Consumers*, which is attached to this Policy as

Exhibit D, should be included with the notice for further guidance on protective measures.

e. A description of what Nursing Service is doing to protect the patient from further Breach and to mitigate the effects of the Breach. To the extent appropriate, alert the patient if notification was delayed due to law enforcement investigation.

f. A method of contacting the Nursing Service to learn more about the Breach. This must be a website, email or mailing address where the public can contact the Nursing Service regarding the Breach. If the Breach includes more than 10 unidentified individuals, the Nursing Service must provide a toll-free number for this purpose.

D. Notify local media outlets, in the following circumstances:

i. If more than 500 Massachusetts residents are affected by the Breach, the Compliance Officer will provide a press release to the media outlets listed below as soon as possible and within 60 days at the latest. The content of the press release should include the same elements as the notification to individuals but should NOT include any personal identifying information. A sample press release is attached to this Policy as Exhibit E.

ii. Media Entities and Contact Information:

1. Boston Globe: email press release to newstip@globe.com.

2. The Acton Beacon:
News Editor – Robert Burgess
978-371-5732
Email: rburgess@cnc.com
Or email beacon@cnc.com

3. Channel 4 (WBZ):
WBZ-TV
1170 Soldiers Field Road
Boston, MA 02134

4. Channel 5 (WCVB):
Andrew Vrees, News Director
WCVB-TV
5 TV Place
Needham, Massachusetts 02494

5. Channel 7 (WHDH): Email: email press release to newstips@whdh.com.

6. Channel 25 (WFXT):
   Lisa Hall, VP, News Director
   WFXT-TV FOX25
   25 Fox Drive
   Dedham, MA 02027-2563

7. WBZ 1030: email press release to
   wbzradionews@wbz1030.com

E. Notify the United States Secretary of Health and Human Services in the following circumstances:

   i. If more than 500 people are affected by the Breach, the Compliance Officer will fill out the electronic form available at http://transparency.cit.nih.gov/breach/index.cfm within 60 days of Breach.
   ii. If fewer than 500 people are affected by the Breach, the Compliance Officer will document the Breach in the attached Breach Information Log (Exhibit F). The Compliance Officer will then fill out an electronic form for each breach using the form available at http://transparency.cit.nih.gov/breach/index.cfm by February 28 of the year following the calendar year in which the Breach occurred.

F. Notify State Officials:

   i. The Compliance Officer will provide a notice to the following as soon as possible after the Breach:

      1. Attorney General Martha Coakley
         Office of the Attorney General
         One Ashburton Place
         Boston, MA 02108

      2. Ms. Barbara Anthony
         Undersecretary
         Office of Consumer Affairs and Business Regulation
         ("OCABR")
         10 Park Plaza –Suite 5170
         Boston, MA 02116

   ii. The notification to the Attorney General and the Undersecretary (also known as the "Director") should include:
      a. A description of the nature of the Breach;
      b. The number of Massachusetts residents affected; and

c. A description of the steps the Nursing Service has taken or plans to take relating to the Breach, including steps taken in order to comply with the HIPAA Breach Notification Rule, the Red Flags Rule, and any other applicable law.

iii. Sample notices to the state officials are attached to this Policy as Exhibit G.

iv. The Office of Consumer Affairs and Business Regulation will notify the Nursing Service of relevant consumer reporting agencies or state agencies that should be contacted. After OCABR provides that information, the Nursing Service should provide a copy of the state notices to the identified agencies.

G. If a patient detects fraudulent activity on an insurance policy or credit account and notifies Nursing Service, the Compliance Officer and Nursing Service will take the following steps:

i. Encourage patient to file a police report.

ii. Encourage patient to complete the *ID Theft Affidavit*, attached to this Policy as Exhibit H and compile supporting documentation.

iii. Compare patient's documentation with personal information in Nursing Service records.

iv. Immediately cease all billing related to the claim in question pending resolution of the question of fraudulent activity.

v. Determine if there is a breach and follow steps for law enforcement, HHS, media, and state agency notification outlined above.

5. Training

A. Staff training will be conducted for all employees, officials and contractors who may come into contact with accounts or personally identifiable information that may constitute a risk to the municipality or the Nursing Service patients. Such employees include employees performing the following tasks:

i. Data entry, coding, or billing;

ii. Handling of charts, referrals, prescriptions or other medical documents;

iii. Contracting or coordination with outside service providers; and

iv. Compliance review for this Policy.

B. The Compliance Officer is responsible for ensuring all employees and contractors conducting the above tasks are properly trained.

C. Employees must receive annual training in all elements of this Policy. Information covered during the annual training will be included in the orientation of newly hired employees.

D. The Compliance Officer will request documentation of training performed or received by Business Associates.

E. To ensure maximum effectiveness, employees will receive additional training as changes to the program are made. Employees and Contactors will receive a copy of any updates to this Policy.

F. Employees will receive a copy of this Policy as part of any annual training. New employees will receive a copy of this Policy during their orientation.

G. Employees who fail to comply with this Policy are subject to sanction as provided by law.

6. Periodic Updates to Plan

A. This Policy will be reevaluated annually by the Compliance Officer to determine whether the program is up to date and applicable given the Nursing Service's practices and the Town of Acton's Master Identity Theft Policy.

B. Periodic reviews will include an assessment of whether new accounts are covered by this Policy and whether existing accounts are susceptible to new forms of Identity Theft.

C. As part of the review, Red Flags may be revised, replaced or eliminated. Defining new Red Flags may also be appropriate. Actions to take in the event that fraudulent activity is discovered may also require revision to reduce damage to the Town and the Nursing Service employees or patients.

D. The Compliance Officer will provide a written report on an annual basis to the Board of Health and Town Manager on the effectiveness of the current Policy and recommended changes for the upcoming year.

E. Revisions to this Policy will be approved by the Board of Health and Board of Selectmen prior to the annual training and signed by the following:

   i. Chairperson of Board of Health;
   ii. Chairperson of Board of Selectmen; and
   iii. Administrator of Nursing Service and Compliance Officer (if different).

7. Oversight of Arrangements with Business Associates

A. The Compliance Officer will ensure that the activities of all Business Associates are conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.

B. As of February 22, 2010, the Business Associates listed in Exhibit 1 currently provide services to the Nursing Service and may have access to the personal data listed in Section C.2. above.

C. Within 30 days of approving this Policy and each January thereafter, the Compliance Officer will request a letter from each Business Associate:

   i. Certifying compliance with the FTC Red Flag Rule, HIPAA Regulations, including the Breach Notification Rule, and Massachusetts Data Privacy rules (if applicable);

ii. Certifying that the Business Associate understands that it is required to notify the Nursing Service of any Breach upon discovery of the Breach; and
iii. Providing a description or copy of the written information security program followed by the Business Associate.

D. The Compliance Officer will review policies of all Business Associates to ensure that they are effective in preventing Identity Theft.

E. The Compliance Officer will provide a copy of this Policy to all Business Associates with a letter requesting that it be followed to the extent it is more stringent than the Business Associates' own policies.

F. When entering into agreements with new Business Associates or renewing existing contracts, the Nursing Service will ensure that the agreement requires compliance with this Policy.

E. APPROVAL AND EFFECTIVE DATE

1. This Policy will take effect immediately upon its approval by the Nursing Service Administrator in consultation with the Group of Professional Personnel, the Board of Health, and the Board of Selectmen.
2. Approval is documented below.

APPROVED:

NURSING SERVICE
ADMINISTRATOR:

The foregoing Policy was approved by vote of the Group of Professional Personnel at a meeting on _____ __, 2010.

_____
By: Merrily Evdokimoff

ACTON HEATLH DIRECTOR:

The foregoing Policy was approved by vote of the Board of Health at an open meeting on _____ __, 2010.

_____
By: Douglas Halley

ACTON BOARD OF SELECTMEN:

The foregoing Policy was approved by vote of the Board of Selectmen at an open meeting on _____ __, 2010.

_____
By: Peter Berry, Clerk

INDEX

EXHIBITS

EXHIBIT	DESCRIPTION
A	Unusual Occurrence Report
B	Breach Assessment Tool
C	Draft Patient Notification Letter
D	*Medical Identity Theft Response Checklist for Consumers*
E	Draft Press Release
F	Sample of Breach Information Log
G	Draft Notification Letter to State Officials
H	Sample of *ID Theft Complaint and Affidavit*
I	List of Business Associates

EXHIBIT A

EXHIBIT A

Acton Public Health Nursing Service

UNUSUAL OCCURRENCE REPORT

To Be Completed by Reporting Employee

Date of incident: _____ Time of incident: _____

Patient/Staff: _____ Phone number: _____

Diagnosis: _____

Physician: _____ Phone number: _____

Family informed of incident? Yes ____ No ____ N/A ____

If yes, who was informed? _____

Physician informed? Yes ____ No ____

By whom? _____

Physician Instructions given? Yes ____ No ____

If yes, comment: _____

_____

Describe incident: _____

_____

_____

_____

_____

_____

_____

_____

Action: _____

_____

_____

_____

_____

Reported by: _____ Date reported: _____ Time: _____

Investigation/follow up: _____

_____

_____

Reviewing
Administrator/Supervisor: _____ Date reviewed: _____ Time: _____

EXHIBIT B

EXHIBIT B

Acton Public Health Nursing Service Breach Assessment Tool

The following questions will help determine whether a breach involving protected health information ("PHI") has occurred that triggers the HIPAA breach notification rule. For further assistance, contact Town Counsel, Stephen Anderson at 617-621-6510 or sanderson@andersonkreiger.com.

	Question	Yes - Next Steps	No - Next Steps
Unsecured PHI			
1	• Was there an impermissible use or disclosure of PHI? • Was the PHI unsecured (i.e.. not rendered unusable, unreadable, indecipherable to unauthorized individuals through the use of encryption technology or similar methodology)?	Continue to next question.	• Notifications are not required. • Document the decision in the breach notification log.
Minimum Necessary			
2	Was more than the minimum necessary PHI for the purpose accessed, used or disclosed?	Continue to next question.	• If you determine there to be a low risk of harm to the individual, do not provide notifications and document the decision in the breach notification log. • Otherwise, continue to next question.
Was there a significant risk of harm to the individual as a result of the impermissible use or disclosure?			
3	Was PHI received and/or used by another entity governed by the HIPAA Privacy & Security Rules or a Federal Agency obligated to comply with the Privacy Act of 1974 & FISA of 2002?	• If you determine there to be a low risk of harm to the individual, do not provide notifications and document the decision in the breach notification log. • Otherwise, continue to next question.	Continue to next question.
4	Were immediate steps taken to mitigate the impermissible use/disclosure such as obtaining the recipients' assurances the information will not be further used or disclosed or will be destroyed?	• If you determine there to be a low risk of harm to the individual, do not provide notifications and document the decision in the breach notification log. • Otherwise, continue to next	Continue to next question.

EXHIBIT B

	Question	Yes - Next Steps	No - Next Steps
		question.	
5	Was the PHI returned before being accessed for an improper purpose? (For example: A laptop is lost or stolen, and then recovered; forensic analysis shows that PHI was not accessed, altered, transferred or otherwise compromised.)	• If you determine there to be a low risk of harm to the individual, do not provide notifications and document the decision in the breach notification log. • Otherwise, continue to next question. • Note: do not delay notifications based on a hope the PHI will be recovered.	Continue to next question.
What type and amount of PHI was involved in the impermissible use or disclosure?			
6	Do the type and amount of PHI pose a significant risk of financial, reputational, or other harm?	**Provide required notifications.**	• If you determine there to be a low risk of harm to the individual, do not provide notifications and document the decision in the breach notification log. • Otherwise, continue to next question.
7	Did the improper use or disclosure of PHI only include the name and the fact services were received?	• If you determine there to be a low risk of harm to the individual, do not provide notifications and document the decision in the breach notification log. • Otherwise, continue to next question.	Continue to next question.
8	Did the improper use or disclosure include the name and type of services received, services were from a specialized facility (such as a substance abuse facility), ***or*** the information increases the risk of ID Theft (such as SS#, account#, mother's maiden name, etc.)?	**Provide required notifications**	Continue to next question.

EXHIBIT B

	Question	Yes - Next Steps	No - Next Steps
9	Is the risk of re-identification so small that the improper use or disclosure poses no significant harm to any individuals? (For example: A limited data set included zip codes that, based on population features, does not create a significant risk an individual can be identified.)	• If you determine there to be a low risk of harm to the individual, do not provide notifications and document the decision in the breach notification log. • Otherwise, continue to next question.	Continue to next question.
Specific Breach Definition Exclusions			
10	Was there an unintentional access, use, or disclosure of PHI by a workforce member acting under the organization's authority, made in good faith, within his/her scope of authority, which did not result in further use or disclosure? (For example, a billing employee receives an e-mail containing PHI about a patient mistakenly sent by a nurse (co-worker). The billing employee alerts the nurse of the misdirected e-mail & deletes it.)	• If you determine there to be a low risk of harm to the individual, do not provide notifications and document the decision in the breach notification log. • Otherwise, continue to next question.	Continue to next question.
11	Was access unrelated to the workforce member's duties? (For example, a receptionist looks through a patient's records to learn of his/her treatment.)	• **Provide required notifications.** • Follow procedures for employee discipline.	Continue to next question.
12	Was there an inadvertent disclosure of PHI by a person authorized to access PHI at the Nursing Service or a Business Associate of the Nursing Service to another person authorized to access PHI at the same organization, or through its organized healthcare arrangement (OHCA), ***and*** the information was not further used or disclosed? (For example: A workforce member who has the authority to use or disclose PHI discloses PHI to another individual in that same organization/OHCA and the PHI is not further used/disclosed.)	• If you determine there to be a low risk of harm to the individual, do not provide notifications and document the decision in the breach notification log. • Otherwise, continue to next question.	Continue to next question.
13	Was a disclosure of PHI made, but there is a good faith belief that the unauthorized recipient would not have reasonably been able to retain it? (For example: EOBs were mistakenly sent to wrong individuals and were returned by the post office, unopened, as undeliverable.) (For example A nurse mistakenly hands a patient discharge papers belonging to a different patient, but quickly realized the mistake and recovers the PHI from the patient, and the nurse reasonable concludes the patient could not have read or otherwise retained the information.)	• If you determine there to be a low risk of harm to the individual, do not provide notifications and document the decision in the breach notification log.	Document findings in the breach notification log. [Note: if the EOBs were not returned as undeliverable, this should be treated as a breach.]

EXHIBIT C

EXHIBIT C -
DRAFT PATIENT NOTIFICATION LETTER

Acton Public Health Nursing Service Draft Breach Notification Letter to Patients – Document to be Customized and Reviewed by the Compliance Officer Prior to Use

[Date]

[Name]
[Address 1]
[Address 2]
[City, State Zip Code]

Dear **[Name]:**

I am writing with important information about a potential breach of your personal information at the Acton Public Health Nursing Service. The circumstances of the incident are as follows:

A. **[Provide a brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.]**
B. **[Provide a description of the types of unsecured personal data or protected health information that were involved in the breach (such as whether full name, Social Security number, date of birth, home address, account number, diagnosis, disability code or other types of information were involved). Do NOT include technical information regarding how the breach occurred as this may further compromise security of personal data.]**
C. **[Describe any steps the individual should take to protect himself or herself from potential harm resulting from the breach.]**
D. **[Provide a brief description of what the organization is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches. Include information regarding criminal complaints filed and cooperation with law enforcement.]**

Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. For your convenience, enclosed is the Federal Trade Commission's ("FTC") recommended *Identity Theft Victim's Complaint and Affidavit*. This form can be used to assist you in filing a criminal complaint if you desire.

Massachusetts law also allows consumers to place a security freeze on their credit reports. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services.

EXHIBIT C -
DRAFT PATIENT NOTIFICATION LETTER

If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift or remove a security freeze. In all other cases, a credit reporting agency may charge you a fee (currently up to $5.00) to place, temporarily lift, or permanently remove a security freeze.

To place a security freeze on your credit report, you must send a written request to **each** of the three major consumer reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and Trans Union (www.transunion.com) by regular, certified or overnight mail to the addresses below (or to an updated address on the referenced websites):

Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348 Phone: 1-800-525-6285	Experian Security Freeze P.O. Box 9554 Allen, TX 75013 Phone: 1-888-EXPERIAN	Trans Union Security Freeze Fraud Victim Assistance Department P.O. Box 6790 Fullerton, CA 92834 Phone: 1-800-680-7289

To request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft; and
8. If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) **and** the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days

after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) **and** the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

In addition, we recommend that you ***immediately*** take the following steps:

- Call the toll-free numbers of any one of the three major credit bureaus (above) to place a fraud alert on your credit report. This can help prevent an identity thief from opening additional accounts in your name. As soon as the credit bureau confirms your fraud alert, the other two credit bureaus will automatically be notified to place alerts on your credit report, and all three reports will be sent to you free of charge.

- Order your credit reports. By establishing a fraud alert, you will receive a follow-up letter that will explain how you can receive a free copy of your credit report. When you receive your credit report, examine it closely and look for signs of fraud, such as credit accounts that are not yours.

- Continue to monitor your credit reports. Even though a fraud alert has been placed on your account, you should continue to monitor your credit reports to ensure an imposter has not opened an account with your personal information.

- Consult the attached *Medical Identity Theft Response Checklist for Consumers* for other steps you can take.

Please call us at (978) 264-9653 during normal business hours with any questions you have. You can also email us at nursing@acton-ma.gov or send us any information by mail at:

Acton Public Health Nursing Service
472 Main St.
Acton, MA 01720

We have also established a section on our website with updated information and links to Web sites that offer information on what to do if your personal information has been compromised. Our website is available at: http://www.acton-ma.gov/index.aspx?nid=153.

EXHIBIT C -
DRAFT PATIENT NOTIFICATION LETTER

We take very seriously our role of helping to safeguard your personal information and using it in an appropriate manner. The Acton Public Health Nursing Services apologizes for the concern this situation may cause you and is taking appropriate steps to help rectify the situation.

Sincerely,

Merrily Evdokimoff, RN, PhD(c)
Administrator
Acton Public Health Nursing Service

cc: Massachusetts Attorney General
Massachusetts Director of Consumer Affairs and Business Regulation
Acton Town Manager
Acton Town Counsel

EXHIBIT D

Medical Identity Theft Response Checklist for Consumers

Consumer awareness is critical for timely detection of and thorough response to a medical identity theft incident. Consumers may follow this checklist for proactive guidance and quick action.

Task		√ When Complete
1.	Explore the resource "Tools for Victims" provided by the Federal Trade Commission (available online at www.ftc.gov/bcp/edu/microsites/idtheft/tools.html). Consider completing the universal affidavit to submit to creditors.	
2.	Review credit reports, correct them, and place a "Fraud Alert" on them.	
3.	If a Social Security number is suspected of being used inappropriately, contact the Social Security Administration's fraud hotline at (800) 269-0721.	
4.	In the case of stolen or misdirected mail, contact the US Postal Service at (800) 275-8777 to obtain the number of the local US Postal Inspector.	
5.	For stolen passports, contact the US Department of State at (877) 487-2778 or http://travel.state.gov.	
6.	If the thief has stolen checks, contact both check verification companies: Telecheck ([800] 366-2425) and the International Check Services Company ([800] 526-5380) to place a fraud alert on the account to ensure that counterfeit checks will be refused.	
7.	Contact the health information manager or the privacy officer at the provider organization or the antifraud hotline at the health plan where the medical identity theft appears to have occurred.	
8.	Request an accounting of disclosures. If the provider or plan refuses access to medical records, file a complaint with the Office for Civil Rights at Health and Human Services at (866) 627-7748 or www.hhs.gov/ocr/privacyhowtofile.htm.	
9.	Take detailed notes of all conversations related to the medical identity theft. Write down the date, name, and contact information of everyone contacted, as well as the content of the conversation.	
10.	Make copies of any letters, reports, documents, and e-mail sent or received regarding the identity theft.	
11.	Work with the organization where the medical identity theft occurred to stop the flow of the incorrect information, correct the existing inaccurate health record entries, and determine where incorrect information was sent.	
12.	File a police report and send copies with correct information to insurers, providers, and credit bureaus once the identity theft has been confirmed.	
13.	File a complaint with the attorney general in the state where the identity theft occurred. The National Association of Attorneys General provides state-by-state information at www.naag.org/attorneys_general.php.	
14.	Check with state authorities for resources. Many states provide consumer protection and education related to insurance and accept online complaints. To determine if a state has a state insurance department for online complaints, visit the National Association of Insurance Commissioners at www.naic.org and file a complaint as appropriate.	
15.	File a complaint with the Identity Theft Data Clearinghouse, operated by the Federal Trade Commission and the Internet Crime Complaint Center. Information available for filing a complaint can be found at https://rn.ftc.gov/pls/dod/widtpubl$.startup?Z_ORG_CODE=PU03.	
16.	Contact the Department of Health and Human Services at (800) 368-1019 or by visiting the Web site at www.hhs.gov/ocr for suspected Medicare or Medicaid fraud.	
17.	Review health records to make sure they have been corrected prior to seeking healthcare.	
18.	Change all personal identification numbers and passwords for protected accounts, sites, access points, etc. Choose unique personal identification numbers and complex passwords rather than common ones (e.g., mother's maiden name, birth date, or pet name).	

EXHIBIT E

EXHIBIT E –
SAMPLE PRESS RELEASE

Acton Public Health Nursing Service
Draft Breach Notification Media Notification Statement/Release –
Document to be Customized and Reviewed by the Compliance Officer Prior to Use

[Insert Date]

Contact: Merrily Evdokimoff, RN, PhD(c)
Administrator
Acton Public Health Nursing Service
472 Main St.
Acton, MA 01720
(978) 264-9653
mevdokimoff@acton-ma.gov.

FOR IMMEDIATE RELEASE

ACTON PUBLIC HEALTH NURSING SERVICE NOTIFIES PATIENTS OF POTENTIAL BREACH OF UNSECURED PERSONAL INFORMATION

The Acton Public Health Nursing Service today notified **[Insert Number]** patients of a potential breach of unsecured personal information after discovering the following event:

A. **[Provide a brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.]**
B. **[Provide a description of the types of unsecured personal information that were involved in the breach (such as whether full name, Social Security number, date of birth, home address, account number, diagnosis, disability code or other types of information were involved).]**
C. **[Describe any steps the individual should take to protect themselves from potential harm resulting from the breach.]**
D. **[Provide a brief description of what the organization is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches.]**
E. **[Provide contact procedures for individuals to ask questions or learn additional information, which includes a toll-free telephone number, an e-mail address, Web site, or postal address.]**

Together with local law enforcement, including the Acton Police Department, the Attorney General's Office, the Office of Consumer Affairs and Business Regulation, and security experts, the Acton Public Health Nursing Service is working to mitigate any potential damage from the incident. The Acton Public Health Nursing Service has in place safeguards to ensure the privacy and security of all patient health information. As a result of this incident, steps are underway to further improve the security of its operations and eliminate future risk.

EXHIBIT E –
SAMPLE PRESS RELEASE

In a notification to patients, the Acton Public Health Nursing Services has identified ways to help patients safeguard information and mitigate any damage resulting from this incident. The Acton Public Health Nursing Service also has encouraged its patients to contact their financial institutions to prevent unauthorized access to personal accounts.

The Acton Public Health Nursing Service has trained staff available for patients to call with any questions related to the incident. Patients may direct any questions to Merrily Evdokimoff, Administrator, Acton Public Health Nursing Service at (978) 264-9653 or nursing@acton-ma.gov. In addition, patients may visit the Nursing Service's Web site at http://www.acton-ma.gov/index.aspx?nid=153 for further information.

The Acton Public Health Nursing Service understands the importance of safeguarding patients' personal information and takes that responsibility very seriously. The Nursing Service will continue to work with patients and law enforcement personnel to ensure the privacy and security of all patient information.

cc: Acton Town Manager
Acton Town Counsel

EXHIBIT F

EXHIBIT F

Acton Public Health Nursing Service Breach Notification Log

The Acton Public Health Nursing Service maintains the following record of any suspected breaches of unsecured protected health information, regardless of the number of patients affected. This log records the investigation of the potential breach and the risk assessment carried out to determine any applicable notification requirements. In the event notification requirements are triggered, a separate incident report will be created and cross–referenced.

Incident #	Date of Discovery	Date of Breach	Location	Brief Description of Breach and Type of Breach Based on Breach Assessment Tool*	Number Patients Involved	Notification Dates			Actions Taken Resolution Steps
						Patients	Media	HHS	

*Describe what happened, including a description of the types of unsecured protected health information that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, etc.). Include the numerical category of Breach based on the Acton Public Health Nursing Service Breach Assessment Tool (Policy Exhibit B).

Year_____ Sheet # _____

EXHIBIT G

EXHIBIT G

Sample Notification Letter to Attorney General's Office – Document to be Customized and Reviewed by Compliance Officer Prior to Use

INTERGOVERNMENTAL COMMUNICATION – May Be Subject to Exemptions (c) (privacy) and (f) (law enforcement) under Public Records Act.

[Date]

BY CERTIFIED MAIL – RETURN RECEIPT REQUESTED

Attorney General Martha Coakley Office of the Attorney General One Ashburton Place Boston, MA 02108	Ms. Barbara Anthony Undersecretary Office of Consumer Affairs and Business Regulations ("OCABR") 10 Park Plaza, Suite 5170 Boston, MA 02116

Dear Attorney General and Undersecretary:

Pursuant to M.G.L. c. 93H, I am writing on behalf of the Acton Public Health Nursing Service to notify you of **[a potential breach of security/an unauthorized access or use of personal information]** involving approximately **[number]** Massachusetts resident**[s]**.

I. NATURE OF THE SECURITY BREACH OR UNAUTHORIZED USE OR ACCESS

[This paragraph should provide:
a. the date of the incident,
b. a summary of the nature of the incident,
c. a description of the categories of personal information involved in the incident, and
d. whether the personal information that was the subject of the incident was in electronic or paper form.]

II. NUMBER OF MASSACHUSETTS RESIDENTS AFFECTED

At this time, the Nursing believes that approximately **[number]** Massachusetts' residents were affected by this incident. All affected residents are being provided a written notice of the incident pursuant to M.G.L. c. 93H, § 3(b) and the HIPAA Breach Notification Rule, 45 CFR Parts 160 and 164. A copy of the notice to affected patients is attached.

[Note: If more than 500 MA residents were involved, also include information about media notification and a copy of the press release.]

EXHIBIT G

III. STEPS THE NURSING SERVICE HAS TAKEN AND PLANS TO TAKE RELATING TO THE INCIDENT

[This paragraph should outline the steps the Nursing Service has taken or plans to take relating to the incident including, without limitation, what the Nursing Service did when it discovered the incident; whether the Nursing Service has any evidence that the personal information has been used for fraudulent purposes; whether the Nursing Service intends to offer credit monitoring services to patients; and what measures the Nursing Service has taken to ensure that similar incidents do not occur in the future.]

The Nursing Service has been in communication with the Acton Police Department regarding the incident. The Police Department is undertaking an investigation of the incident to determine the source and extent of the potential breach. **[If applicable, include a description of any delay requested by law enforcement].**

IV. FURTHER INFORMATION

The Acton Public Health Nursing Service is taking this incident very seriously and will work with your office, the Office of Consumer Affairs and Business and Business Regulations, the Acton Police Department and affected patients to mitigate the potential for further harm from this incident. If you have any questions regarding the incident or need further information please contact me at (978) 264-9653 or mevdokimoff@acton-ma.gov. I appreciate your support in addressing this matter.

Sincerely,

Merrily Evdokimoff, RN, PhD(c)
Administrator
Acton Public Health Nursing Service

cc: Acton Town Manager
Acton Town Counsel

EXHIBIT H

Average time to complete: 10 minutes

Identity Theft Victim's Complaint and Affidavit

A voluntary form for filing a report with law enforcement, and disputes with credit reporting agencies and creditors about identity theft-related problems. Visit ftc.gov/idtheft to use a secure online version that you can print for your records.

Before completing this form:

1. Place a fraud alert on your credit reports, and review the reports for signs of fraud.
2. Close the accounts that you know, or believe, have been tampered with or opened fraudulently.

About You *(the victim)*

Now

(1) My full legal name: _____
First Middle Last Suffix

(2) My date of birth: _____
mm/dd/yyyy

(3) My Social Security number: _____-_____-_____

(4) My driver's license: _____ _____
State Number

(5) My current street address:

_____
Number & Street Name Apartment, Suite, etc.

_____
City State Zip Code Country

(6) I have lived at this address since _____
mm/yyyy

(7) My daytime phone: (____)_____
My evening phone: (____)_____
My email: _____

Leave (3) blank until you provide this form to someone with a legitimate business need, like when you are filing your report at the police station or sending the form to a credit reporting agency to correct your credit report.

At the Time of the Fraud

(8) My full legal name was: _____
First Middle Last Suffix

(9) My address was: _____
Number & Street Name Apartment, Suite, etc.

_____
City State Zip Code Country

(10) My daytime phone: (____)_____ My evening phone: (____)_____
My email: _____

Skip (8) - (10) if your information has not changed since the fraud.

About You (the victim) (Continued)

Declarations

(11) I ☐ did OR ☐ did not authorize anyone to use my name or personal information to obtain money, credit, loans, goods, or services — or for any other purpose — as described in this report.

(12) I ☐ did OR ☐ did not receive any money, goods, services, or other benefit as a result of the events described in this report.

(13) I ☐ am OR ☐ am not willing to work with law enforcement if charges are brought against the person(s) who committed the fraud.

About the Fraud

(14) I believe the following person used my information or identification documents to open new accounts, use my existing accounts, or commit other fraud.

(14): Enter what you know about anyone you believe was involved (even if you don't have complete information).

Name: _____
First Middle Last Suffix

Address: _____
Number & Street Name Apartment, Suite, etc.

_____
City State Zip Code Country

Phone Numbers: (____)_____ (____)_____

Additional information about this person: _____

(15) Additional information about the crime (for example, how the identity thief gained access to your information or which documents or information were used):

(14) and (15): Attach additional sheets as needed.

_____

_____

_____

_____

_____

_____

_____

Documentation

(16) I can verify my identity with these documents:

(16): Reminder: Attach copies of your identity documents when sending this form to creditors and credit reporting agencies.

☐ A valid government-issued photo identification card (for example, my driver's license, state-issued ID card, or my passport).
If you are under 16 and don't have a photo-ID, a copy of your birth certificate or a copy of your official school record showing your enrollment and legal address is acceptable.

☐ Proof of residency during the time the disputed charges occurred, the loan was made, or the other event took place (for example, a copy of a rental/lease agreement in my name, a utility bill, or an insurance bill).

About the Information or Accounts

(17) The following personal information (like my name, address, Social Security number, or date of birth) in my credit report is inaccurate as a result of this identity theft:

(A) _____

(B) _____

(C) _____

(18) Credit inquiries from these companies appear on my credit report as a result of this identity theft:

Company Name: _____

Company Name: _____

Company Name: _____

(19) Below are details about the different frauds committed using my personal information.

Name of Institution | Contact Person | Phone | Extension

Account Number | Routing Number | Affected Check Number(s)

Account Type: ☐ Credit ☐ Bank ☐ Phone/Utilities ☐ Loan
☐ Government Benefits ☐ Internet or Email ☐ Other

Select ONE:
☐ This account was opened fraudulently.
☐ This was an existing account that someone tampered with.

Date Opened or Misused (mm/yyyy) | Date Discovered (mm/yyyy) | Total Amount Obtained ($)

Name of Institution | Contact Person | Phone | Extension

Account Number | Routing Number | Affected Check Number(s)

Account Type: ☐ Credit ☐ Bank ☐ Phone/Utilities ☐ Loan
☐ Government Benefits ☐ Internet or Email ☐ Other

Select ONE:
☐ This account was opened fraudulently.
☐ This was an existing account that someone tampered with.

Date Opened or Misused (mm/yyyy) | Date Discovered (mm/yyyy) | Total Amount Obtained ($)

Name of Institution | Contact Person | Phone | Extension

Account Number | Routing Number | Affected Check Number(s)

Account Type: ☐ Credit ☐ Bank ☐ Phone/Utilities ☐ Loan
☐ Government Benefits ☐ Internet or Email ☐ Other

Select ONE:
☐ This account was opened fraudulently.
☐ This was an existing account that someone tampered with.

Date Opened or Misused (mm/yyyy) | Date Discovered (mm/yyyy) | Total Amount Obtained ($)

---

(19):
If there were more than three frauds, copy this page blank, and attach as many additional copies as necessary.

Enter any applicable information that you have, even if it is incomplete or an estimate.

If the thief committed two types of fraud at one company, list the company twice, giving the information about the two frauds separately.

Contact Person: Someone you dealt with, whom an investigator can call about this fraud.

Account Number: The number of the credit or debit card, bank account, loan, or other account that was misused.

Dates: Indicate when the thief began to misuse your information and when you discovered the problem.

Amount Obtained: For instance, the total amount purchased with the card or withdrawn from the account.

Your Law Enforcement Report

(20) One way to get a credit reporting agency to quickly block identity theft-related information from appearing on your credit report is to submit a detailed law enforcement report ("Identity Theft Report"). You can obtain an Identity Theft Report by taking this form to your local law enforcement office, along with your supporting documentation. Ask an officer to witness your signature and complete the rest of the information in this section. It's important to get your report number, whether or not you are able to file in person or get a copy of the official law enforcement report. Attach a copy of any confirmation letter or official law enforcement report you receive when sending this form to credit reporting agencies.

Select ONE:

- ☐ I have not filed a law enforcement report.
- ☐ I was unable to file any law enforcement report.
- ☐ I filed an automated report with the law enforcement agency listed below.
- ☐ I filed my report in person with the law enforcement officer and agency listed below.

(20):
Check "I have not..." if you have not yet filed a report with law enforcement or you have chosen not to. Check "I was unable..." if you tried to file a report but law enforcement refused to take it.

Automated report:
A law enforcement report filed through an automated system, for example, by telephone, mail, or the Internet, instead of a face-to-face interview with a law enforcement officer.

_____
Law Enforcement Department State

_____ _____
Report Number Filing Date (mm/dd/yyyy)

_____
Officer's Name (please print) Officer's Signature

_____ _____
Badge Number Phone Number

Did the victim receive a copy of the report from the law enforcement officer? ☐ Yes OR ☐ No

Victim's FTC complaint number (if available): _____

Signature

As applicable, sign and date *IN THE PRESENCE OF* a law enforcement officer, a notary, or a witness.

(21) I certify that, to the best of my knowledge and belief, all of the information on and attached to this complaint is true, correct, and complete and made in good faith. I understand that this complaint or the information it contains may be made available to federal, state, and/or local law enforcement agencies for such action within their jurisdiction as they deem appropriate. I understand that knowingly making any false or fraudulent statement or representation to the government may violate federal, state, or local criminal statutes, and may result in a fine, imprisonment, or both.

_____ _____

Signature Date Signed (mm/dd/yyyy)

Your Affidavit

(22) If you do not choose to file a report with law enforcement, you may use this form as an Identity Theft Affidavit to prove to each of the companies where the thief misused your information that you are not responsible for the fraud. While many companies accept this affidavit, others require that you submit different forms. Check with each company to see if it accepts this form. You should also check to see if it requires notarization. If so, sign in the presence of a notary. If it does not, please have one witness (non-relative) sign that you completed and signed this Affidavit.

_____

(Notary)

Witness:

_____ _____

(signature) (printed name)

_____ _____

(date) (telephone number)

EXHIBIT I

EXHIBIT I

Acton Public Health Nursing Service: Business Associates

Business Associate	Service Provided	Contact Name	Contact Address	Contact Phone/Email	Business Associate Agreement Start Date	Contract End Date
Healthwyse, LLC	Software	Steve Booth, VP	60 Concord St., Wilmington, MA 01887	877-777-9973	April 14, 2003	Current
Ansaphone Service, Inc.	Answering Service	Will Porter, Director of Sales & Marketing	1212 Hancock St. Quincy, MA 02169	800-782-7587	February 9, 2008	Current

Sheet # _____